The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
06/15/2011

SUBJECT:
Vulnerability in Adobe Flash Player Could Allow For Remote Code Execution (APSB11-18)

OVERVIEW:
A vulnerability has been discovered in Adobe Flash Player which could allow attackers to take complete control of affected systems. Adobe Flash Player is a widely distributed multimedia and application player used to enhance the user experience when visiting web pages or reading email messages. Successful exploitation will cause the application to crash and could also result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

It should be noted that this vulnerability is being exploited on the Internet in targeted attacks via malicious Web pages.

SYSTEMS AFFECTED:
- Adobe Flash Player 10.3.181.23 and earlier versions for Windows, Macintosh, Linux and Solaris operating systems
- Adobe Flash Player 10.3.185.23 and earlier versions for Android
- Flash Player integrated with Google Chrome

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: **High**

DESCRIPTION:
A memory corruption vulnerability has been discovered for Adobe Flash Player that could cause the system to crash and potentially allow the attacker to run code in the context of the user running the application. This vulnerability may be exploited if a user opens a specially crafted Adobe Flash file by visiting a web site.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

It should be noted that this vulnerability is being exploited on the Internet in targeted attacks via malicious Web pages.

RECOMMENDATIONS:
The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Inform and educate users regarding the threats posed by hypertext links contained in emails, IM (Instant Messages) or attachments especially from un-trusted sources.

REFERENCES:

Adobe:
http://www.adobe.com/support/security/bulletins/apsb11-18.html

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2110

Security Focus:
http://www.securityfocus.com/bid/48268